



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

1/1

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/775,205	02/01/2001	Alan Boate	RIDM.P-002	7111
32692	7590	02/17/2006	EXAMINER	
3M INNOVATIVE PROPERTIES COMPANY PO BOX 33427 ST. PAUL, MN 55133-3427			SHIFERAW, ELENI A	
		ART UNIT	PAPER NUMBER	
			2136	

DATE MAILED: 02/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/775,205	BOATE ET AL.
Examiner	Art Unit	
Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 12 December 2005.

2a) This action is FINAL. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-21 is/are pending in the application.
4a) Of the above claim(s) 22 is/are withdrawn from consideration.
5) Claim(s) _____ is/are allowed.
6) Claim(s) 1-21 is/are rejected.
7) Claim(s) _____ is/are objected to.
8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 04/11/2001 is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
5) Notice of Informal Patent Application (PTO-152)
6) Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/12/2005 has been entered.
2. Claims 1-21 are presented for examination.
3. Claim 22 has been canceled.

Specification

4. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

With regards to the abstract, the length clearly exceeds the 150 word suggested maximum length.

Drawings

5. New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because the handwritten parts of the drawings are hard to interpret. Applicant is

advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claim 1-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Scott et al. (Scott, U.S. Patent No. 6,484,260) in view of Davis (U.S. Patent No. 5,568,552) and Addy (U.S. Patent No. 6,255,944 B1).

Regarding claims 1, 9, and 17, Scott et al. teaches a method/security system for controlling access to a computer network at a network access point comprising a workstation, said system comprising:

- a personal digital identifier device (fig. 1, ref. num 6) comprising:
 - a wireless communications component comprising a transceiver (fig. 1, ref. num 26 and 28 and col. 6, lines 52-53),

a biometric acquisition component for obtaining a user's input biometric and producing a digital representation thereof (fig. 1, ref. num 11, 12, 14, and 15 and col. 6, lines 41-47),

a processor configured for communicating with said transceiver and said biometric component (fig. 1, ref. num 16, 18, 20, 22, and 23) and operable for:

evaluating whether a template derived from said digital representation corresponds to a master template derived from a user's biometric digital representation previously produced by said biometric component and generating a matching signal when such a correspondence is determined (col. 10, lines 15-29),

generating a private key to be held by said personal digital identifier device and a public key corresponding thereto and outputting said generated public key for transmission by said transceiver (col. 10, lines 50-55),

secure storage containing said master template of a user's biometric, said generated private key (fig. 1, ref. num 20 and col. 8, lines 34-36),

said personal digital identifier device being configured for producing, using said generated private key, a challenge response message following said generating of said matching signal in response to a challenge received from said security manager component and for transmitting said response message (col. 2, lines 28-39), and

said personal digital identifier device being configured to prevent transmission of any of said master template of a user's biometric and said private key (col. 11, lines 56-59),

- a base unit associated with said workstation and configured for initiating and maintaining wireless communications with said personal digital identifier device (fig. 1, ref. num 4, 8, 38, and 40),
said communications extending over an area defined by an envelope associated with said workstation (col. 10, lines 58-63), and,
 - a central server having access to network storage and utilizing said security manager component and said personal digital identifier device for authenticating said user (fig. 1, ref. num 32, 34, and 36),
said network storage containing a public key corresponding to said private key generated by said personal digital identifier device (col. 7, lines 2431).

Scott does not teach a processor used for: producing a digital signature using said private key and, verifying that an encrypted received message is from a security manager component using a public key for a private key associated with said security manager component; the secure storage containing said public key for said private key associated with said security manager component; and the challenge response message is digitally signed.

Davis teaches:

- a processor used for:
producing a digital signature using said private key (col. 5, lines 27-30) and,

verifying that an encrypted received message is from a security manager component using a public key for a private key associated with said security manager component (col. 4, lines 54-65);

- the secure storage containing said public key for said private key associated with said security manager component (col. 4, lines 40-53); and
- the challenge response message is digitally signed (col. 4, lines 3-10).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a processor used for: producing a digital signature using said private key and, verifying that an encrypted received message is from a security manager component using a public key for a private key associated with said security manager component; the secure storage containing said public key for said private key associated with said security manager component; and the challenge response message is digitally signed, as taught by Davis, with the method/system of Scott.

It would have been obvious to combine the steps taught by Davis, with the method/system of Scott because the digital signature and digitally signed response message provide non-repudiation from the PDI to the base unit; this enables the base unit to trust that the PDI in question is the PDI that is supposed to be used. Storing the public key of the security manager in the secure storage area of the PDI, which corresponds to the private key stored in the security manager, to verify encrypted received messages enables the PDI to verify the base units identity. Any encrypted message sent from the security manager to the PDI can be checked for non-repudiation by using the corresponding public key that is stored in the PDI.

Scott and Davis teach all the subject matter as described above. **Scot discloses a user of PDI approaching an ATM/base unit. Once the user is within a certain distance, the exchanging of ID codes and authenticating of the PDI user occurs. Only after a successful authentication will the user be able to see information displayed of the ATM. No information is displayed for non-authorized/not registered PDI user.**

However Scott and Davis fail to explicitly disclose whereby a policy manager component may direct that the screen of said workstation be **blanked out** when a new personal digital identifier device moves to a location within said envelope until such time as the user registered to said personal digital identifier device is biometrically identified.

Addy teaches the well-known method of blanking a display from unauthorized mobile user accessing/viewing sensitive contents (see, col. 8 lines 1-4).

It would have been obvious to one ordinary skill in the art at the time of the invention was made to employ the teachings of blanking out a display with in Scott's not providing any sensitive data when a new/unauthorized PDI device user enters to a location proximity because it very well known to blank out a screen from unknown users for access control security. One would have been motivated to do so because it would not provide/display sensitive information to unauthorized PDI device user.

Regarding claims 2 and 10, Scott as modified by Davis and Addy teaches wherein said biometric component includes a transducer (see col. 1, lines 66-67 of Scott).

Regarding claims 3 and 12, Scott et al. as modified by Davis and Addy teaches wherein said base unit regularly transmits a first signal to said personal digital identifier device and said personal digital identifier device automatically transmits a response signal in response thereto when said personal digital identifier device is within said envelope (see col. 10, lines 58-65 of Scott).

Regarding claims 4 and 14, Scott et al. as modified by Davis and Addy teaches wherein all data held in said secure storage is by itself non-identifiable of said user (see col. 8, lines 34-38 of Scott).

Regarding claim 5, Scott et al. as modified by Davis and Addy teaches wherein said transducer comprises a solid-state fingerprint sensor (see col. 6, lines 54-66 of Scott).

Regarding claim 6, Scott et al. as modified by Davis and Addy teaches wherein said transceiver transmits and receives optical signals (see col. 7, lines 35-50 of Scott).

Regarding claim 7, Scott et al. as modified by Davis and Addy teaches wherein said transceiver transmits and receives radio frequency signals (see col. 7, lines 35-50 of Scott).

Regarding claim 8, Scott et al. as modified by Davis and Addy teaches in combination with a device holder wherein said device holder is configured to co-operate with said housing of said personal digital identifier device such that said personal digital identifier device is held by said holder device when it is appropriately positioned relative to said holder device (see fig. 5B, ref. num 58). The Examiner takes Official Notice for said device holder comprising a communications connector for communicatively coupling said personal digital identifier device

directly to one said workstation when said personal digital identifier device is held by said device holder.

Personal digital identifiers consist of small handheld devices, such as a PDA or other small electronic device. The use of a device holder, which communicatively couples the PDI with a workstation, is an obvious modification, since the device holder would service as a 'dock' to simultaneously allow the PDI to be connected to the workstation and charge the battery of the PDI.

Regarding claim 11, Scott et al. as modified by Davis and Addy teaches wherein said workstation is a personal computer (see col. 6, lines 31-34 of Scott).

Regarding claims 13 and 19, Scott et al. as modified by Davis and Addy teaches comprising a plurality of said personal digital identifier devices, a plurality of workstations and a plurality of base units wherein a base unit is associated with each said workstation (see col. 6, lines 29-40 and col. 11, lines 46-59 of Scott, *each customer has a PDI, each ATM is connected to a bank office, wherein the ATM is the base unit and the bank office is the workstation*), each said base unit transmitting a polling signal to each said personal digital identifier device within said base unit's associated envelope following said base unit's receipt of said response signal from each said personal digital identifier device (see col. 10, lines 58-65 of Scott).

Regarding claims 15 and 20, Scott et al. as modified by Davis and Addy teaches wherein said network storage includes data identifiable of said user for display on a screen of said workstation

when said user's personal identification device is located within said envelope (see col. 10, line 58 through col. 11, line 33 of Scott).

Regarding claims 16 and 18, Scott et al. as modified by Davis and Addy teaches wherein said envelope has a shape and area which are configured to encompass those locations proximate to said workstation at which an observer may read and/or understand information displayed on a screen of said workstation (see col. 9, lines 29-38 and col. 10, lines 58-63 of Scott).

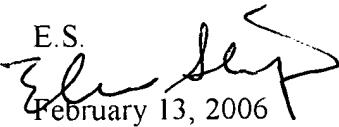
Regarding claim 21, Scott et al. as modified by Davis and Addy teaches further comprising initially registering said user by a registrar in the presence of a guarantor, said registrar and guarantor each being a registered user of the computer network and said registrar having access to the computer network and verified by said security manager component to have registration privileges, and requiring that said guarantor provide to said security manager component a biometrically digitally signed message to authenticate said guarantor and that each of said registrar, guarantor and user remain within said envelope during said registering of said user (see col. 11, lines 46-59 of Scott).

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E.S.

February 13, 2006


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100